Extending Zero Trust to The Data Layer

Cigent, a Duo Technology Partner specializing in software and firmware-based data security solutions, chose Duo's adaptive secure access to protect sensitive data at scale.

THE CHALLENGE:

Defending Data at All Times

Protecting data is more important than ever. Ransomware attacks, loss of IP, and data breaches can negatively impact an organization financially and reputationally, and sophisticated threat actors are constantly refining their strategies to bypass existing protections in order to steal and ransom sensitive data. This reality calls for a new approach to data defense, one that protects data from virtually all threat vectors by placing protections as close to the attack surface as possible, defending data at all times, even when networks or systems are compromised.

Cigent, a Duo Technology Partner, addressed this issue by integrating Duo's adaptive secure access to prevent the financial and reputational loss due to advanced cyberattacks, helping organizations secure their sensitive files even in the event of a breach.

Cigent's Data Defense solution, combined with Duo Security, now part of Cisco, extends Duo's multi-factor authentication to require zero trust access to sensitive files, external media, and internal storage on Windows PCs. This integration ensures sensitive files are always protected by Duo MFA in a simple way that is far more effective than other solutions and protects files from theft, insider threat, and ransomware.

Duo + Cigent: Extending Zero Trust to The Data Layer

Duo Trust Monitor creates a baseline of normal user and device access within a corporate environment. Deviations from this baseline can be used to highlight suspicious activity like account takeover. Visibility into normal and atypical access patterns also enables stronger, more granular access policy.
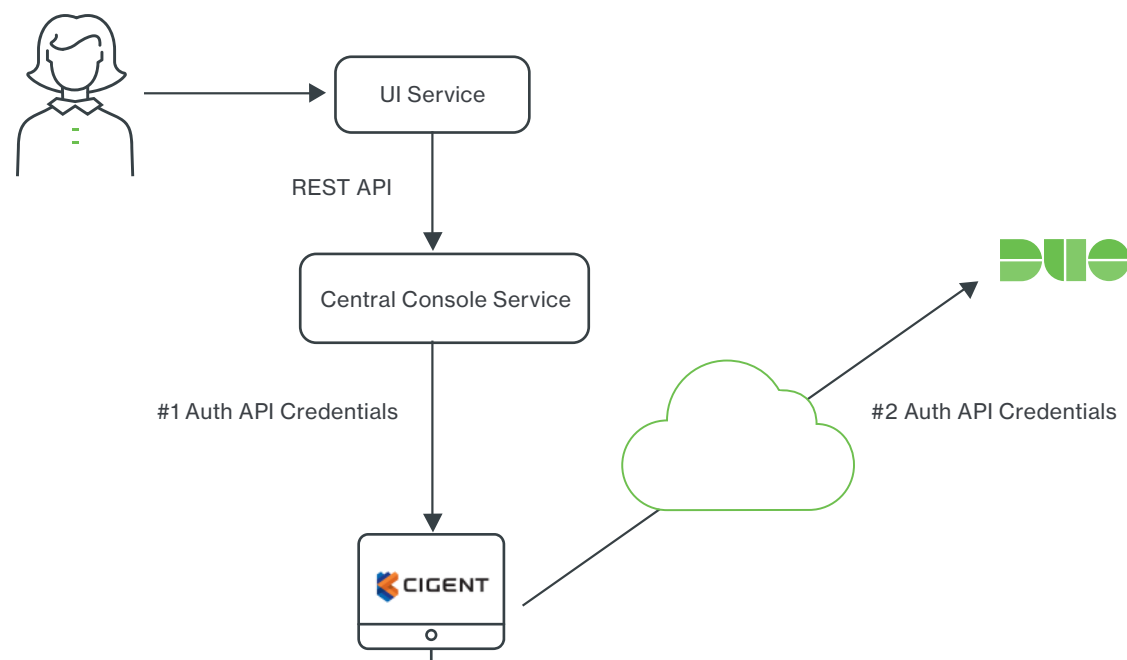
About Duo

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo is a trusted partner to more than 25,000 customers globally, including Bird, Facebook, Lyft, University of Michigan, Yelp, Zillow and more. Try it for free at duo.com.

About Cigent

Cigent specializes in software and firmware-based data security solutions that protect sensitive files from ransomware and data theft throughout the entire data life cycle. For more information, visit cigent.com.

Duo Adaptive Authentication and MFA

Our user-friendly zero trust platform provides three key benefits to help organizations of all sizes protect sensitive data at scale:

01

Zero Trust Access Controls

Cigent D3E adds Duo authentication for access to any sensitive file as well as Cigent Secure SSDs. Duo verifies the identity of the user, ensuring that only trusted users may access sensitive files. This protects against data theft, ransomware, and insider threats, even when user credentials have been stolen or the system compromised.

02

Strong MFA Protection for Encrypted File Access

The combination of Cigent D3E with Duo's adaptive secure access and Cigent Secure SSD (external media or internal storage), protects organizations against many threat vectors including fileless malware, supply chain attacks, below-the-OS attacks such as kernel and hypervisor attacks, chip implants, boot/rootkits, firmware/BIOS malware, as well as credential compromise, software vulnerabilities, and more. When a system has Cigent Secure SSD, granular Secure Drives can be created to encrypt sensitive files and keep them hidden away from threat actors at all times until the user mounts them with Duo MFA. While mounted, if a threat is detected, the O/S locks, or the PC shuts down. Secure Drives automatically encrypt all files and disappear from the OS layer. Once encrypted, the only way to unlock a Secure Drive is with D3E using Duo.

03

Active Lock Threat Response

Cigent D3E is threat-aware and integrates with Cisco Secure Endpoint, along with other endpoint protection solutions, to monitor for attacks on PCs. When a threat is detected, Active Lock protects designated files and Cigent Secure Drives, requiring Duo for access, until the threat is cleared.